Zeggenschap over lichaamsmateriaal

Prins, J.E.J.

Published in:
Nederlands Juristenblad

Publication date:
2013

Document Version
Publisher's PDF, also known as Version of record

Zorgplichten en Cybercrime

18 De maand april maakte wel heel duidelijk hoe kwetsbaar en afhankelijk de populariteit van digitale dienstverlening ons heeft gemaakt. Tegoeden op bankrekeningen verdwenen in de virtuele wereld als sneeuw voor de zon, internetwinkels leden naar eigen zeggen tientallen miljoenen euro's schade omdat het betaalsysteem iDeal niet functioneerde, de KLM was uit de lucht voor wie comfortabel online wilde inchecken en ook de overheidsauthenticatiedienst DigiD werd getroffen. Oorzaak: zogenaamde Denial-of-Service-aanvallen (DoS-aanval). Hierbij wordt de normale capaciteit van systemen, onlinediensten en/of infrastructuur aangevallen doordat kwaadwillenden deze overladen met dataverkeer en daarmee overbelasten. Het gevolg is dat de websites, mailservers en daarmee online diensten niet meer of slecht bereikbaar zijn voor legitiem dataverkeer. Was een DoS-aanval vijftien jaar geleden niet meer dan een vorm van vandalisme zonder duidelijke strategie, inmiddels is dat wel anders. De acties kennen nu specifieke doelen: afpersen van bedrijven, een afleidingsmanoeuvre om spionage en criminele activiteiten te verhullen of het dwars zitten van tegenstanders (repressieve regimes zetten het instrument in tegen opposanten). Steeds vaker ook blijken DoS-aanvallen te worden benut als moderne vorm van protest. Tot nu toe waren bij het publiek vooral de aanvallen op websites bekend. Maar de recente voorvallen laten zien dat ook andere doelwitten mogelijk zijn, zoals infrastructuur voor digitale betaaltransacties. Duidelijk is ook dat de aanvallen steeds vaker zijn gericht op digitale omgevingen die een grote maatschappelijke zichtbaarheid hebben of relevant zijn voor de vitale sectoren (niet alleen financiele diensten, maar ook energie- en drinkwatervoorziening).

De getroffen bedrijven hebben aangifte gedaan, maar de kans is klein dat de daders worden gepakt. Ondertussen zien diverse partijen zich geconfronteerd met miljoenen euro's schade en ligt de vraag voor wie deze gaat betalen. Als het aan Eurocommissaris Kroes ligt komen de banken in beeld: "Kapitaalkrachtige partijen als banken moeten aansprakelijk gehouden kunnen worden voor schade door cybercriminaliteit." Voormalig minister van Defensie Van Middelkoop, nu kwartiermaker voor de Cybersecurity Academy, merkte in het FD op: "Het is genant dat banken ons massaal aan het interbankieren hebben gekregen en we nu moeten constateren dat ze de zaken niet op orde hebben". Maar de voorzitter van de Nederlandse Vereniging van Banken (NVvB), Boele Staal, liet al direct weten dat compensatie niet aan de orde is, omdat sprake is van overmacht. De banken doen 'er alles aan' om de dreiging te pareren. Maar wat is 'er alles aan doen' als het aankomt op de te nemen maatregelen om het uitvallen van (betalings)netwerken te voorkomen? Waren de genomen maatregelen - binnen de grenzen van het redelijke - wel 'voldoende'? Dat verlangt een discussie over de vraag welke risico's bij een DoS-aanval de aanbieder van online diensten vallen toe te rekenen en dus wanprestatie oplevert (art 6:74 BW) en in welke situaties de omstandigheden zodanig zijn dat ze een overmachtsituatie rechtvaardigen (artikel 6:75 BW)?

Belangrijk is hierbij dat in de jurisprudentie van banken een grotere mate van zorgvuldigheid wordt verwacht dan de normale contractuele standaard. De Hoge Raad wijst op de 'rol die banken in het maatschappelijk verkeer vervullen' (HR 29 september 1995, *NJ* 1998, 81). Gegeven de sleutelfunctie die banken spelen in het maatschappelijk en economisch verkeer, moet de samenleving erop kunnen vertrouwen dat zij het toevertrouwde betalingsverkeer correct en betrouwbaar uitvoeren. Nu digitale diensten en elektronische transacties een enorme vlucht hebben genomen – waar banken actief hun rol in hebben gespeeld – zou het dramatische gevolgen hebben voor de economie als bedrijven en particulieren het digitale bankwezen niet langer vertrouwen. Kortom, de zorgplicht die op banken rust brengt mee dat zij meer dan het normale doen als het op de continuïteit en betrouwbaarheid van hun digitale dienstverlening aankomt. Voor toezichthouder DNB kan hier – vanuit de specieke opdracht van het *oversight*toezicht – wel eens nadrukkelijk een rol zijn weggelegd.

Wie op de berichtgeving in de media afgaat, kan zich niet aan de indruk onttrekken dat er bij het bedrijfsleven sprake is van een gebrek aan 'awareness' als het op digitale bedreigingen aankomt. Deze constatering zet de nodige druk op de mogelijkheden om een beroep te doen op overmacht. De ellende en daaruit voortvloeiende schade betreft dan immers veel meer de gevolgen van de keuze niet te handelen, dan een gebeurtenis die zich in belangrijke mate aan beïnvloeding van deze bedrijven onttrok. In hoeverre een onvoldoende alertheid bij banken een rol heeft gespeeld bij de recente systeemuitval is (nog) onduidelijk. Maar voor toekomstige aanvallen lijkt op voorhand het argument van overmacht niet langer valide. Natuurlijk is het voor bedrijven moeilijk pro-actief tot een goede risico-inschatting van en daarmee maatregelen tegen een mogelijke DoS-aanval te komen, onder meer omdat de ernst van de dreiging sterk afhankelijk is van het type aanvaller en diens motieven. Bovendien lokt de ene ellende de andere uit: andere kwaadwillenden proberen vaak een graantje mee te pikken van de verwarring na een DoS-aanval (de aanval op de banken leidde tot meer pogingen tot phishing - ontfutselen van wachtwoorden en inlognamen van rekeninghouders). Maar overmacht of niet: de 'wake up call' van april moet op z'n minst worden opgevat als een stevig signaal aan bedrijven en organisaties hun zorgplichten en daarmee verantwoordelijkheden serieus te nemen. Maar ook is het een signaal richting de juridische praktijk en het maatschappelijke en politieke debat om cyberveiligheid niet langer uitsluitend vanuit strafrechtelijke opsporing van daders te benaderen, maar ook te bediscussiëren vanuit civielrechtelijke zorgplichten voor dienstenaanbieders, de rol van zelfregulering daarbij en wellicht zelfs de implicaties van een en ander voor strafrechtelijke aansprakelijkheid.

Corien Prins

Reageer op NJBlog.nl op het Vooraf.